RECEIVED
CENTRAL FAX CENTER

OCT 16 2006

REMARKS

The following remarks are made in response to the Office Action mailed July 14, 2006. Claims 1-28 were rejected. With this Response, claims 1-13 and 25-27 have been amended. Claims 1-28 remain pending in the application and are presented for reconsideration and allowance.

Claim Objections

The Examiner objected to "at least one of revoked by the certificate authority and expired." language in claims 1 and 13. Amended independent claims 1 and 13 are clarified to recite that the issued certificates are each not signed by the certificate authority and are each valid until at least one of revoked by the certificate authority and expired. Thus, according to amended independent claims 1 and 13 each issued certificate is valid until at least one of: 1) revoked by the certificate authority and 2) expired.

In view of the above, Applicant respectfully requests that the objections to claims 1 and 13 be removed.

Claim Rejections under 35 U.S.C. § 112

The Examiner rejected claims 1-28 under 35 U.S.C. § 112, second paragraph.

The Examiner rejected claims 1-28 because the term "PKI" is stated in the claims along with unsigned documents. The Examiner suggested that the public key infrastructure (PKI) be amended to public key system or unsigned public key infrastructure to overcome the § 112 rejection. Amended claims 1-13 and 25-27 change "public key infrastructure (PKI)" to "public key system."

In view of the above, claims 1-28 are believed to be in form for allowance. Therefore, Applicant respectfully requests that rejections to these claims under 35 U.S.C. § 112, second paragraph, be reconsidered, and that the rejections be removed and these claims be allowed.

Claim Rejections under 35 U.S.C. § 103

The Examiner rejected claims 1, 2, 6, 7, 8, 13, 14, 18, 19, 20, 25, and 26 under 35 U.S.C. 103(a) as being unpatentable over the Smith U.S. Patent No. 6,651,166 in view of the "How PGP works" reference in view of the Fischer U.S. Patent No. 5,475,826.

The Examiner rejected claims 3, and 15 under 35 U.S.C. 103(a) as being unpatentable over the Smith U.S. Patent No. 6,651,166 in view of the "How PGP works" reference in view of the Fischer U.S. Patent No. 5,475,826 in view of the Stallings reference "How to protect the company jewels".

The Examiner rejected claims 4 and 16 under 35 U.S.C. 103(a) as being unpatentable over the Smith U.S. Patent No. 6,651,166 in view of the "How PGP works" reference in view of the Fischer U.S. Patent No. 5,475,826 in view of the Maruyama U.S. Patent 6,393,563.

The Examiner rejected claims 5 and 17 under 35 U.S.C. 103(a) as being unpatentable over the Smith US 6,651,166 in view of the "How PGP works" reference in view of the Fischer U.S. Patent No. 5,475,826 in view of the Kausik U.S. Patent No. 6,263,446.

The Examiner rejected claims 9, 21, 27, and 28 under 35 U.S.C. 103(a) as being unpatentable over the Smith U.S. Patent No. 6,651,166 in view of the "How PGP works" reference in view of the Fischer U.S. Patent No. 5,475,826 in view of the Gasser U.S. Patent No. 5,224,163.

The Examiner rejected claims 10 and 22 under 35 U.S.C. 103(a) as being unpatentable over the Smith U.S. Patent No. 6,651,166 in view of the "How PGP works" reference in view of the Fischer U.S. Patent No. 5,475,826 in view of the Micali U.S. Patent No. 5,793,868 in view of the Boyle U.S. Patent No. 6,212,636.

The Examiner rejected claims 11 and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over the Smith U.S. Patent No. 6,651,166 in view of the "How PGP works" reference in view of the Fischer U.S. Patent No. 5,475,826 in view of the Micali U.S. Patent No. 5,793,868 in view of the Boyle U.S. Patent No. 6,212,636 in view of the Perlman U.S. Patent No. 5,687,235.

The Examiner rejected claims 12 and 24 under 35 U.S.C. 103(a) as being unpatentable over the Smith U.S. Patent No. 6,651,166 in view of the "How PGP works" reference in view of the Fischer U.S. Patent No. 5,475,826 in view of the Micali U.S. Patent

No. 5,793,868 in view of the Boyle U.S. Patent No. 6,212,636 in view of the Gasser U.S. Patent No. 5,224,163.

Amended independent claims 1 and 13 are not taught or suggested by the combination of the Smith et al. patent, the "How PGP works" reference, and the Fischer patent.

Amended independent claims 1 and 13 include limitations of a certificate authority issuing a first certificate to a subject, the first certificate including a public key of the subject, long-term identification information related to the subject, and meta-data related to the first certificate, wherein the first certificate is not signed by the certificate authority. The certificate authority maintains a database of records representing issued certificates in which it stores a record representing the first certificate, wherein the issued certificates are each not signed by the certificate authority and are each valid until at least one of revoked by the certificate authority and expired. Amended independent claims 1 and 13 further recite that a verifier maintains a hash table containing cryptographic hashes of valid certificates corresponding to the records stored in the database and including a cryptographic hash of the first certificate.

The Smith et al. patent, the "How PGP works" reference, and the Fischer patent alone or in combination do not teach or suggest a verifier maintaining a hash table containing cryptographic hashes of valid certificates wherein issued certificates are each not signed by the certificate authority and are each valid until at least one of revoked by the certificate authority and expired, wherein the hash table includes a cryptographic hash of the first certificate having a public key of the subject, long-term identification information related to the subject, and meta-data related to the first certificate, wherein the first certificate is not signed by the certificate authority as recited in amended independent claims 1 and 13.

As admitted by the Examiner, the Smith et al. patent and the "How PGP works" reference do not teach a verifier maintaining cryptographic hashes. Furthermore, the Fischer patent teaches a system that maintains hashes of **files** in a security database not a verifier maintaining a hash table containing cryptographic hashes of **valid certificates**, wherein issued certificates are each not signed by the certificate authority and are each valid until at least one of revoked by the certificate authority and expired and the hash table includes a cryptographic hash of the first certificate including a public key of the subject, long-term

identification information related to the subject, and meta-data related to the first certificate, wherein the first certificate is not signed by the certificate authority.

In addition, the Smith et al. does not teach or suggest a certificate authority issuing unsigned certificates. The Smith et al. patent specifically states, at column 2, lines 39-41, "[a] digital certificate, as disclosed later, is a record of a public key and an identity, and the association of the two as attested to by a third party by means of a digital signature." Figure 9 of the Smith et al. patent is a simplified diagram of a digital certificate that does not show the digital signature, because the digital signature is not a new component in the Smith et al. sender driven certification enrollment system. The Smith et al. patent later states, at column 7, lines 12-14, that "[s]ome of the components, such as the certificate server 88 do not require any customization or development." Thus, the Smith et al. patent does not teach or suggest issuing certificates that are each not signed by the certificate authority as required by the limitations of amended independent claims 1 and 13.

Conventional public key cryptography systems, such as the public key cryptography systems disclosed in the "How PGP works" reference, typically provide that the certificate authority issue signed certificates and the recipient of the signed certificate calculate the hash code of the unsigned certificate and compare this to the hash code recovered from the signed certificate. If the two codes match, this is a valid certificate and the recipient may trust the public key in that the signed certificate belongs to the identified user. Whereas defined by amended independent claims 1 and 13, the certificate authority issues certificates that are each not signed by the certificate authority and are each valid until at least one of revoked by the certificate authority and expired, the certificate authority maintains a database of records representing issued certificates, and the verifier maintains a hash table containing certificate of hashes of valid certificates corresponding to the records stored in the database and includes a cryptographic hash of the first certificate, wherein the subject presents the issued first certificate to the verifier for authentication and demonstrates that the subject has knowledge of a private key corresponding to the public key of the first certificate. In this way, the invention defined by amended independent claims 1 and 13 permits a means by which public keys can be managed on a secure basis for use by widely distributed users or systems without the normal expensive mechanism of having a certificate authority issue a signed certificate.

In view of the above, amended independent claims 1 and 13 are not taught or suggested by the combination of the Smith et al. patent, the "How PGP works" reference, and the Fischer patent. As dependent claims 2-12 and 25-27 further define patentably distinct amended independent claim 1; and as dependent claims 14-24 and 28 further define patentably distinct amended independent claim 13, these dependent claims are also believed to be allowable.

Therefore, Applicant respectfully requests reconsideration and withdrawal of the 35 U.S.C. § 103 rejections to claims 1-28 and allowance of these claims.

CONCLUSION

In view of the above, Applicant respectfully submits that pending claims 1-28 are in form for allowance and are not taught or suggested by the cited references. Therefore, reconsideration and withdrawal of the rejections and allowance of claims 1-28 is respectfully requested.

No fees are required under 37 C.F.R. 1.16(h)(i). However, if such fees are required, the Patent Office is hereby authorized to charge Deposit Account No. 08-2025.

The Examiner is invited to contact the Applicant's representative at the below-listed telephone numbers to facilitate prosecution of this application.

Any inquiry regarding this Amendment and Response should be directed to either Patrick G. Billig at Telephone No. (612) 573-2003, Facsimile No. (612) 573-2005 or Kevin Hart at Telephone No. (970) 898-7057, Facsimile No. (970) 898-7247. In addition, all correspondence should continue to be directed to the following address:

IP Administration
Legal Department, M/S 35
HEWLETT-PACKARD COMPANY
P.O. Box 272400
Fort Collins, Colorado 80527-2400

Respectfully submitted,

Francisco Corella

By his attorneys,

DICKE, BILLIG & CZAJA, PLLC
Fifth Street Towers, Suite 2250
100 South Fifth Street
Minneapolis, MN 55402
Telephone: (612) 573-2003
Facsimile: (612) 573-2005

Date: 10-16-06

Patrick G. Billig
Reg. No. 38,080

CERTIFICATE UNDER 37 C.F.R. 1.8:

The undersigned hereby certifies that this paper or papers, as described herein, are being transmitted via facsimile to Facsimile No. (571) 273-8300 on this 16 day of October, 2006.

By: _____
Name: Patrick G. Billig